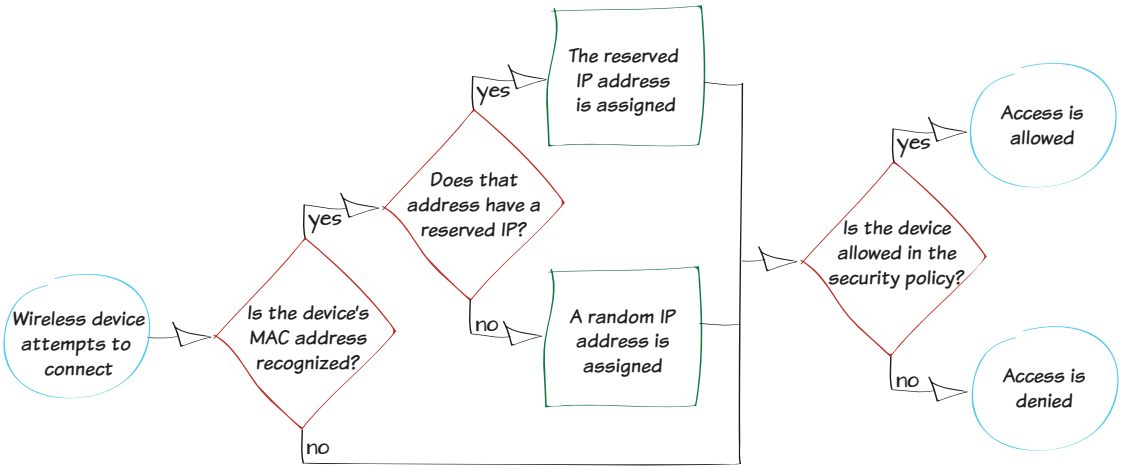
Using MAC access control to allow access to the wireless network

In this example, you will add device definitions to your FortiGate using Media Access Control (MAC) addresses. These definitions are then used to determine which devices can access the wireless network.

By using a MAC address for identification, you will also be able to assign a reserved IP for exclusive use by the device when it connects to the wireless network.

Since MAC addresses can be easily spoofed, using MAC access control should not be considered a security measure.

1. Finding the MAC address of a device
2. Defining a device using its MAC address
3. Creating a device group
4. Reserving an IP address for the device
5. Creating a security policy for wireless traffic
6. Results



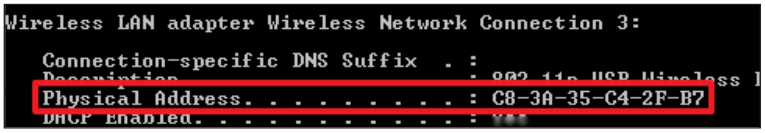
1. Finding the MAC address of a device

The instructions below were written for the most recent OS versions. Older versions may use different methods.

For Windows devices:

Open the command prompt and type `ipconfig /all`.

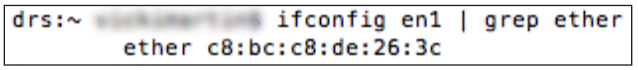
This output displays configuration information for all of your network connections. Look for the information about the wireless adapter and take note of the **Physical Address**.



For Mac OS X devices:

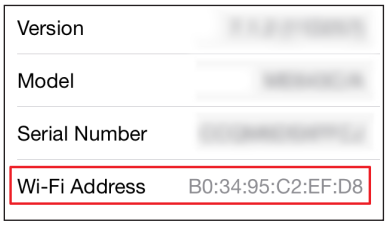
Open **Terminal** and type `ifconfig en1 | grep ether`.

Take note of the displayed MAC address.



For iOS devices:

Open **Settings > General** and take note of the **Wi-Fi Address**.



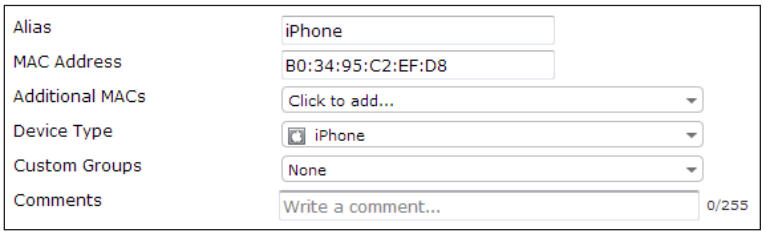
For Android devices:

Open **Settings > More > About Device > Status** and take note of the **Wi-Fi MAC address**.

2. Defining a device using its MAC address

Go to **User & Device > Device > Device Definitions** and create a new device definition.

Set **MAC Address** to the address of the device and set the other fields as required. In the example, a device definition is created for an iPhone with the MAC Address B0:34:95:C2:EF:D8.



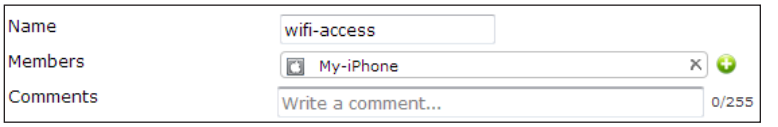
The new definition will now appear in your device list.

If you have enabled device identification on the wireless interface, device definitions will be created automatically. You can then use MAC addresses to identify which device a definition refers to.

3. Creating a device group

Go to **User & Device > Device > Device Groups** and create a new group.

Add the new device to the **Members** list.

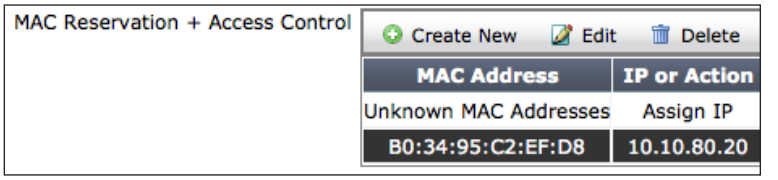


4. Reserving an IP address for the device

Go to **System > Network > Interfaces** and edit the wireless interface.

Under **DCHP Server**, expand **Advanced**. Create a new entry in the **MAC Reservation + Access Control** list that reserves an IP address within the DCHP range for the device's MAC address.

If the FortiAP is in bridge mode, you will need to edit the internal interface.

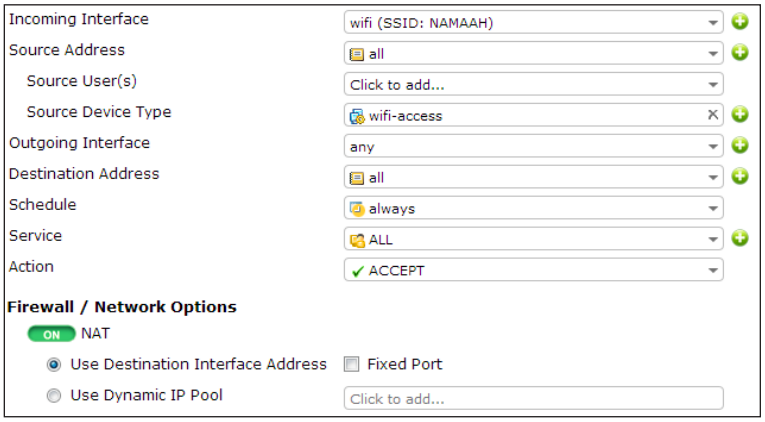


5. Creating a security policy for wireless traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your wireless interface, **Source Device Type** to the device group, and **Outgoing Interface** to the Internet-facing interface.

Ensure that **NAT** is turned on.

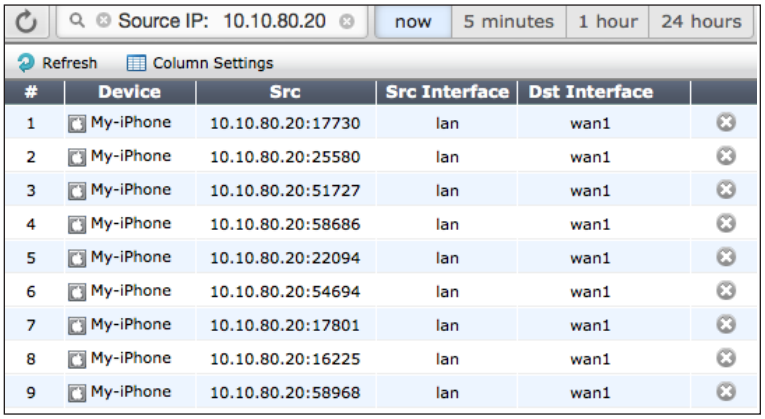


6. Results

Connect to the wireless network with a device that is a member of the device group. The device should be able to connect and allow Internet access.

Connection attempts from a device that is not a group member will fail.

Go to **System > FortiView > All Sessions** and view the results for **now**. Filter the results using the reserved Source IP (in the example, 10.10.80.20), to see that it is being used exclusively by the wireless device.



#	Device	Src	Src Interface	Dst Interface
1	My-iPhone	10.10.80.20:17730	lan	wan1
2	My-iPhone	10.10.80.20:25580	lan	wan1
3	My-iPhone	10.10.80.20:51727	lan	wan1
4	My-iPhone	10.10.80.20:58686	lan	wan1
5	My-iPhone	10.10.80.20:22094	lan	wan1
6	My-iPhone	10.10.80.20:54694	lan	wan1
7	My-iPhone	10.10.80.20:17801	lan	wan1
8	My-iPhone	10.10.80.20:16225	lan	wan1
9	My-iPhone	10.10.80.20:58968	lan	wan1